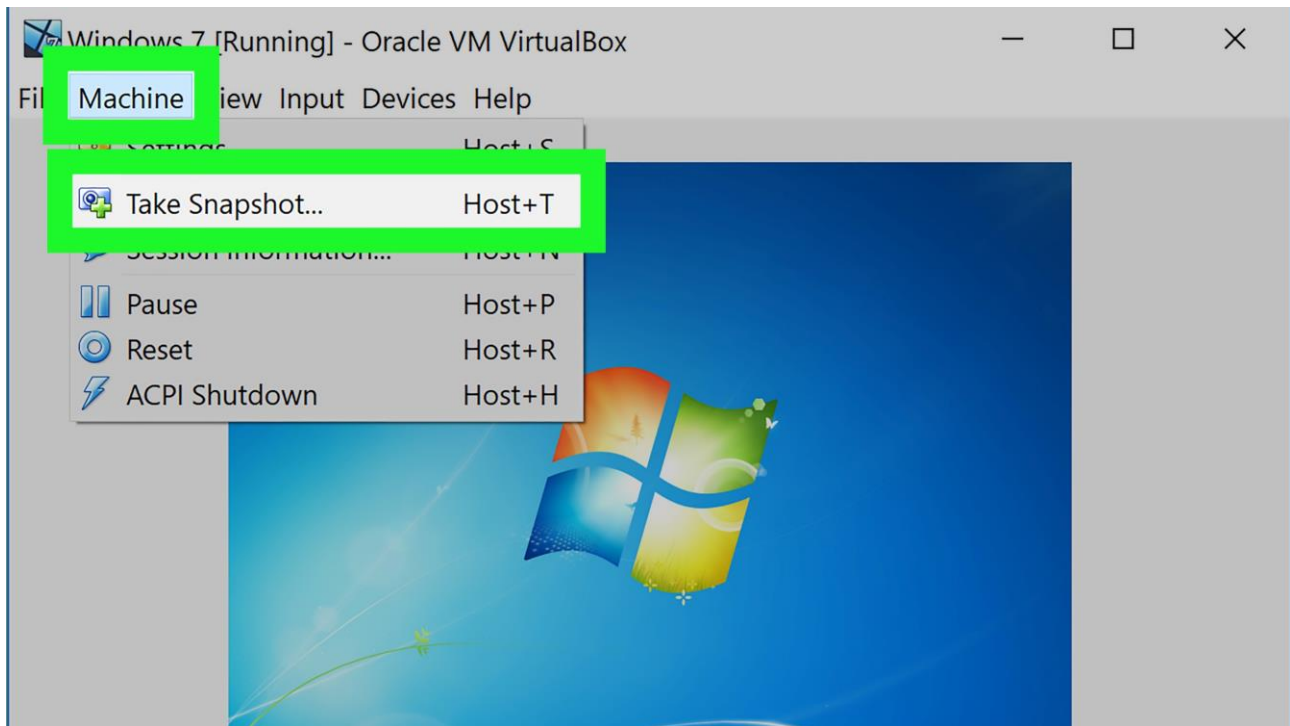


Per monitorare le attività di malware sul file system, in particolare le chiamate alla funzione `CreateFile` su path noti (come il path dell'eseguibile del malware), possiamo seguire questi passaggi:

**1. Creazione di un'istantanea della macchina VirtualBox:**

- Aprire VirtualBox e selezionare la macchina Windows XP.
- Fare clic su "Macchina" -> "Istantanea" -> "Prendi istantanea".
- Dare un nome e una descrizione all'istantanea per ricordare lo stato della macchina in quel momento.



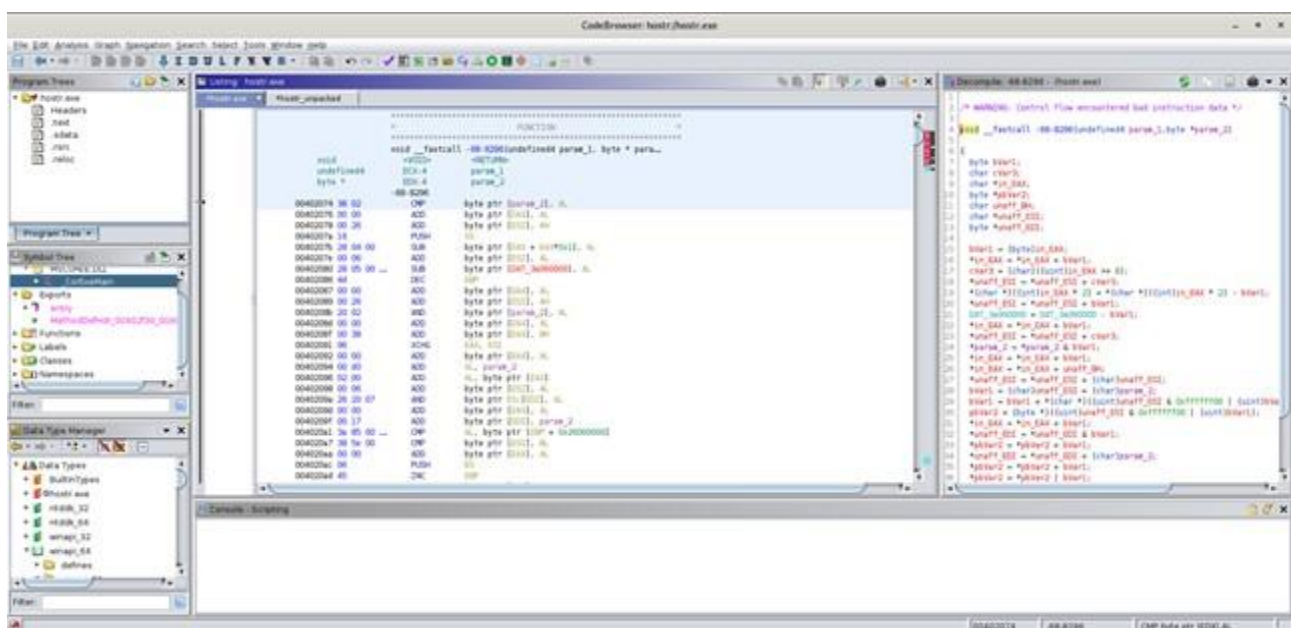
**Monitoraggio delle chiamate alla funzione `CreateFile`:**

- Scaricare e installare strumenti di monitoraggio come Process Monitor (Procmon) di Sysinternals.
- Configurare Process Monitor per monitorare le chiamate a `CreateFile`.
  - Aprire Process Monitor.
  - Applicare un filtro per le chiamate `CreateFile`:
    - Fare clic su "Filter" -> "Filter..." (o premere Ctrl+L).
    - Aggiungere una nuova regola: "Operation" -> "is" -> "CreateFile" -> "Include".
    - Aggiungere un'altra regola per il path dell'eseguibile del malware, se noto: "Path" -> "contains" -> "<path\_to\_malware>" -> "Include".
    - Fare clic su "Add" e poi su "OK" per applicare i filtri.

Process Monitor - Sysinternals: www.sysinternals.com										
File Edit Event Filter Tools Options Help										
Time ...	Process Name	Sess...	PID	Arch...	Operation	Path	Result	Detail	Date & Time	Image Path
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS		5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM	SUCCESS	Desired Access: M...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegQueryValue	HKLM	SUCCESS	Query: HandleTag...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM\system\Setup	SUCCESS	Desired Access: R...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM	SUCCESS		5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupIn...	SUCCESS	Type: REG_DWO...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS		5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM	SUCCESS	Desired Access: M...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegQueryValue	HKLM	SUCCESS	Query: HandleTag...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM\system\Setup	SUCCESS	Desired Access: R...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM	SUCCESS		5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupIn...	SUCCESS	Type: REG_DWO...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS		5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,766,144...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,864,448...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 11,190,272...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,856,256...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,749,760...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,897,216...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,782,528...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,823,488...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,807,104...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,733,376...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 23,044,096...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,880,832...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,692,416...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,651,456...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,889,024...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 22,036,480...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 23,543,808...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,790,720...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,774,336...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,954,560...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,643,264...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 20,332,544...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,757,952...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,921,792...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,831,680...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,848,064...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM	SUCCESS	Desired Access: M...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegQueryValue	HKLM	SUCCESS	Query: HandleTag...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM\system\Setup	SUCCESS	Desired Access: R...	5/25/2021 12:42:...	C:\Windows\sysste...

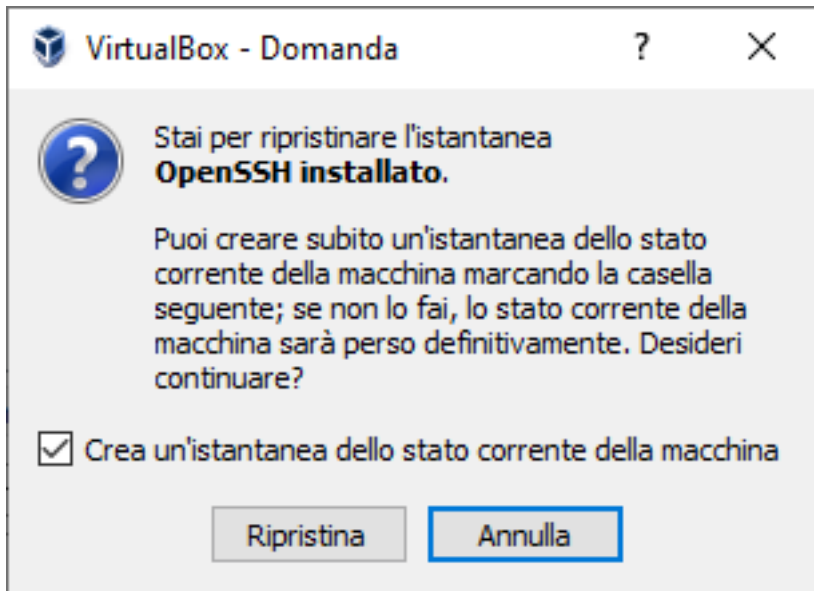
## Analisi del malware:

- Eseguire il malware in un ambiente controllato.
- Osservare e registrare tutte le chiamate `CreateFile` nel path specificato.
- Analizzare i risultati per determinare le attività sospette o malevole.



## Ripristino della macchina:

- Dopo aver completato l'analisi, è possibile ripristinare lo stato della macchina virtuale utilizzando l'istantanea creata precedentemente.
  - Selezionare la macchina virtuale in VirtualBox.
  - Fare clic su "Macchina" -> "Istantanea" -> selezionare l'istantanea e fare clic su "Ripristina".



## Alternativa: Clonazione della macchina virtuale

1. **Clonare la macchina virtuale:**
  - Fare clic destro sulla macchina virtuale e selezionare "Clona"

